

## UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

FILED  
MAY 23 2025  
JOAN KANE, CLERK  
U.S. DIST. COURT WESTERN DIST. OKLA.  
BY [initials] DEPUTY

## In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

A BLACK IPHONE WITH 2 CAMERAS ON THE BACK  
LOCATED AT THE CHICKASAW LIGHHOUSE POLICE  
DEPARTMENT, WITHIN THE WESTERN DISTRICT OF  
OKLAHOMA

Case No. M-25-344-AMG

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A," which is attached and incorporated by reference herein.

located in the Western District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B," which is attached and incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

## Code Section

## Offense Description

18 U.S.C. § 2252A(a)(5)(B)

Possessing or Accessing with Intent to View Material Containing Child Pornography

18 U.S.C. § 2252A(a)(2)

Distribution or Receipt of Child Pornography

The application is based on these facts:

See attached Affidavit of CLPD Investigator Isaac Bates, which is incorporated by reference herein.

Continued on the attached sheet.

Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
\_\_\_\_\_  
Applicant's signature

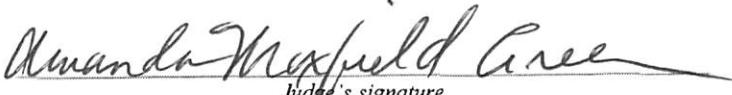
ISAAC BATES, CLPD INVESTIGATOR

Printed name and title

Sworn to before me and signed in my presence.

Date: 5/23/25

City and state: Oklahoma City, Oklahoma

  
\_\_\_\_\_  
AMANDA MAXFIELD GREEN, U.S. MAGISTRATE JUDGE  
Judge's signature

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF A  
BLACK IPHONE WITH 2 CAMERAS ON  
THE BACK LOCATED AT THE  
CHICKASAW LIGHHOUSE POLICE  
DEPARTMENT, WITHIN THE WESTERN  
DISTRICT OF OKLAHOMA

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Isaac Bates, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a Search Warrant authorizing the examination of property—an electronic Device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. Affiant is a Criminal Investigator for the Chickasaw Lighthorse Police Department (CLPD). Your Affiant is currently assigned to the Oklahoma State Bureau of Investigations Internet Crimes Against Children's Task Force (OSBI ICAC). Your Affiant has been employed by the Chickasaw Lighthorse Police Department since February of 2022. Your Affiant began his career with the Denison Police Department in Denison, Texas, in 2007, working as a patrol officer, conducting several basic patrol functions and investigating various crimes. In 2014, your Affiant began his employment with the Grayson County Sheriff's Office in Sherman, Texas, and became a Criminal Investigator from 2015 to 2019. During this time, your Affiant was assigned to Sexual Assault investigations and Child Sexual Assault crimes, including cases of Child Sexual Abuse Material (CSAM). During Affiant's time as a Law Enforcement Officer and Criminal Investigator,

Affiant has participated in numerous criminal investigations as the primary investigator or in a backup capacity. Affiant has also received significant training in criminal investigations, including investigations into violent crimes, Sexual Assault Investigations, and computer crimes.

3. As a Law Enforcement Officer, Affiant, has received approximately 2350 hours of Continuing Education from the Texas Commission on Law Enforcement (TCOLE) and held an Advanced Peace Officer License in Texas prior to transferring to Oklahoma and is currently licensed with the Oklahoma Council on Law Enforcement Education and Training (CLEET).

4. As a Criminal Investigator with the CLPD, your affiant is a law enforcement officer of the Chickasaw Nation, as well as a special commissioned law enforcement officer (SLEC) with the Bureau of Indian Affairs (BIA). Your affiant is also a United States law enforcement officer as defined by 18 U.S.C. § 2510(7), meaning that your Affiant is empowered by law to conduct investigations of and to make arrests for violations of Federal law, including violations of the Major Crimes Act (MCA).

5. For the purposes of supporting this Application for Search Warrant, I have set forth herein facts that I believe are sufficient to establish probable cause to believe that evidence of violations of 18 U.S.C § 2252A(a)(5)(B) (Possessing or Accessing with Intent to View Material Containing Child Pornography), 18 U.S.C § 2252A(a)(2) (Distribution or Receipt of Child Pornography) are located in the following device seized during an arrest of Zachary Lee White in Midwest City, Oklahoma on May 13, 2025: **a Black iPhone with 2 cameras on the back. No visible damage or identifying numbers, hereinafter referred to as the “TARGET DEVICE.”**

6. The TARGET DEVICE is further described in Attachment A. The TARGET DEVICE is currently secured at the Chickasaw Nation Police Department, located in the Western District of Oklahoma. The applied-for Warrant would authorize the forensic examination of the

**TARGET DEVICE** for the purpose of identifying electronically stored data, particularly described in Attachment B.

7. The information in this Affidavit is based upon my personal knowledge, training, and experience, and information learned, either directly or indirectly, from witnesses, records, and other law enforcement officers and agents. This Affidavit is intended to show merely that there is sufficient probable cause for the requested Warrants and does not set forth all my knowledge about this matter.

**PROBABLE CAUSE FACTS**

8. On April 22, 2024, I received a case from OSBI ICAC task force and began an investigation into Zachary Lee WHITE's involvement in the possession and distribution of Child Pornography (CLPD Case #2024-11354). The investigation began when OSBI received a cybertip from the National Center for Missing and Exploited Children (NCMEC) associated with what appeared to be WHITE's Snapchat account. Eventually, a total of three cybertips, alleging the presence or transfer of Child Sexual Abuse Material (CSAM) over the internet, were received from NCMEC and are associated with either WHITE's phone number, email, or both.

9. On April 22, 2024, I reviewed cybertip #188544129 that involved a Snapchat account with telephone number (405)695-9524, username "red\_slayer69420," and a user date of birth of 10/10/1992. OSBI ICAC analysts previously determined through a TLO open record search that telephone number (405)695-9524 was connected to Zachary Lee WHITE, date of birth of 10/10/1992, who lived at 1669 Cowboy LN, Blanchard, Oklahoma. On April 22, 2024, I also verified this information via an open-source search. I reviewed the images associated with the cybertip and confirmed that the images were CSAM. One image depicted a young prepubescent female engaged in sexually explicit conduct with, what appeared to be, a white female with a strap-on dildo. One image depicted a prepubescent female engaged in sexually explicit activity with a

dark-skinned male. According to the cybertip, these images were uploaded or transferred using the subject Snapchat account on February 29, 2024.

10. On July 3, 2024, I reviewed cybertip #189649823 that involved an Instagram account with username “red\_slayer2022” and email of “zachary6673@gmail.com.” OSBI ICAC analysts previously determined through an open record search that email “Zachary6673@gmail.com” to be associated with Zachary Lee WHITE. I reviewed one of the images that was uploaded to or transferred from this Instagram account and confirmed that it was CSAM. This image depicted two prepubescent females both ~~bare~~<sup>naked</sup> <sup>amc</sup> from the waist down exposing their vaginal area. According to the cybertip, several CSAM images were uploaded or transferred using the subject Instagram account on March 14, 2024, and March 15, 2024.

11. Cybertip #193635146 involved a Discord account with username “luckyshot2913” and email “zachary6673@gmail.com.” I reviewed the image that was uploaded to or transferred from this ~~Instagram~~<sup>Discord</sup> <sup>amc</sup> account and confirmed that it was CSAM. This image depicted a prepubescent nude male engaged in sexually explicit conduct with a prepubescent nude female laying on her back with her legs in the air. According to the cybertip, this image was uploaded or transferred using the subject Discord account on May 15, 2024.

12. On July 18, 2024, a Chickasaw Nation search warrant was executed at WHITE’s residence at 1669 Cowboy Ln, Blanchard, Oklahoma and the following devices were seized: 1) WHITE’s iPhone 12 Pro Max, 2) WHITE’s Acer laptop, 3) WHITE’s son’s iPhone SE, 4) WHITE’s son’s HP laptop. Upon review of the devices, no CSAM was found to be present on the devices. However, upon a search of the mail application on WHITE’s iPhone 12 Pro Max, an email was sent from Discord to “zachary6673@gmail.com” on June 22, 2022, stating, “you have 9 new messages.” There was also an email from Discord to “zachary6673@gmail.com” notifying

WHITE that his Discord account had violated community standards, which was likely related to the NCMEC cybertip discovery of CSAM on WHITE's Discord account.

13. On July 18, 2024, I interviewed WHITE regarding the NCMEC cybertips. WHITE confirmed that the email "zachary6673@gmail.com" belonged to him. WHITE also confirmed that his phone number is (405)695-9524. WHITE claimed that he does not have any social media other than Facebook. WHITE explained that he used to have Snapchat a year ago with username "luckyshot2913."

14. On May 13, 2025, WHITE was arrested by the United States Marshall Service pursuant to a federal arrest warrant in case number CR-25-167-PRW. Upon being arrested, a mobile cellular device (**TARGET DEVICE**) was located in WHITE'S possession and seized as evidence to be later forensically examined.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO TRANSPORT,  
DISTRIBUTE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD  
PORNOGRAPHY**

15. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books,

slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.<sup>1</sup>

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Bateman uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

16. In light of the aforementioned, including the facts that demonstrate WHITE possessed, accessed with intent to view, distributed, and/or received child pornography through

<sup>1</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "stolenness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

his Snapchat, Instagram, and Discord accounts, and based on my training and experience, I believe that there is probable that evidence of such criminal activity will be found on the TARGET DEVICE.

### **TECHNICAL TERMS**

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Snapchat: Snapchat is a mobile application that provides users a way to share photos, videos, and chats.
- b. Instagram: Instagram is a free photo and video sharing app available on iPhone and Android. People can upload photos or videos to our service and share them with their followers or with a select group of friends. They can also view, comment and like posts shared by their friends on Instagram. Anyone 13 and older can create an account by registering an email address and selecting a username.
- c. Discord: Discord is a multimedia messaging application that provides chat and messaging functions to its users, as well as servers and channels that allow users to share messages, files, and other content through messaging and voice channels.
- d. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- e. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also

include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- f. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- g. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude, with a high level of precision.
- h. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- i. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for

example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

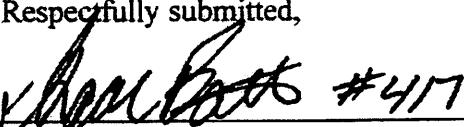
- j. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- k. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- l. Sexually Explicit Conduct: Sexually Explicit Conduct is defined in 18 U.S.C. § 2256(2) as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

18. Based on my training, experience, and research, I know that the **TARGET DEVICE** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, and/or tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

**CONCLUSION**

24. I understand that no warrant shall issue, but upon probable cause and upon particularly describing the place to be searched and the things to be seized. I submit that there is sufficient reason to believe, based on the evidence described above, that the **TARGET DEVICE** further described in Attachment A, contains evidence related to the possession, accessing with intent to view, distribution, or receipt of Child Pornography. Thus, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **TARGET DEVICE** to seek the items described in Attachment B.

Respectfully submitted,

  
Isaac Bates

Criminal Investigator  
Chickasaw Lighthorse Police Department

Subscribed and sworn to before me on May 23, 2025.

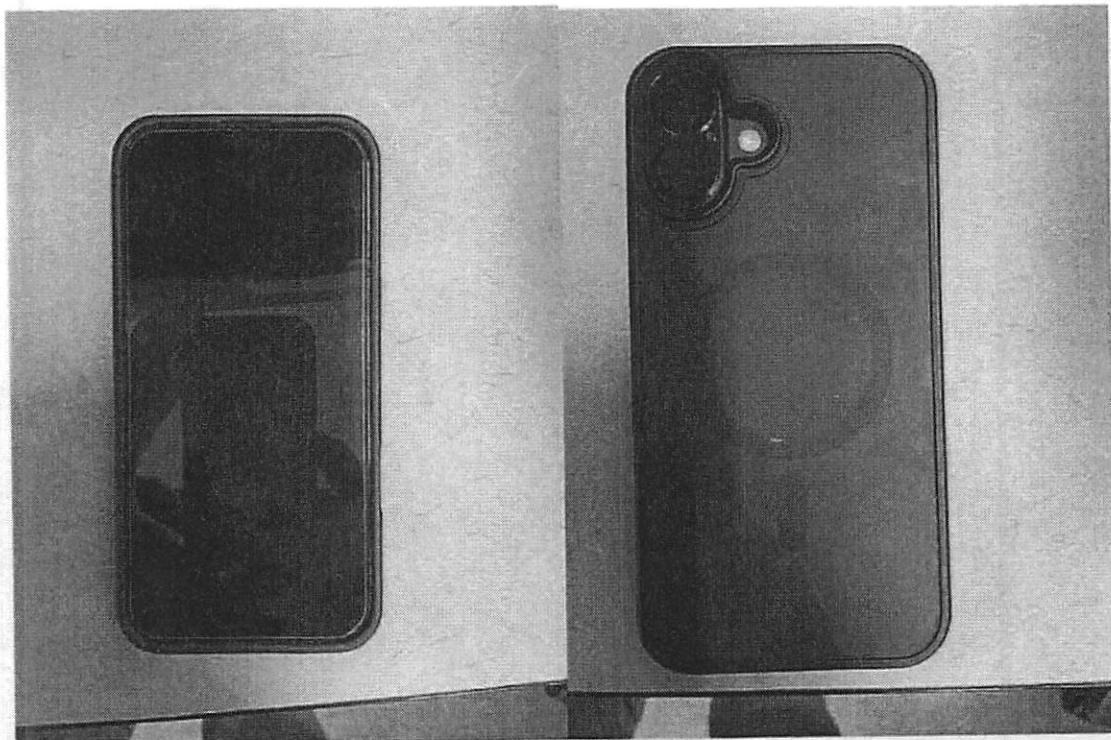
  
AMANDA MAXFIELD GREEN  
United States Magistrate Judge

**ATTACHMENT A**

The property to be searched is a **Black iPhone with 2 cameras on the back with no visible damage or identifying numbers.**

The **TARGET DEVICE** is currently located at the Chickasaw Lighthorse Police Department, within the Western District of Oklahoma. Below are photographs of the **TARGET DEVICE**.

This Warrant authorizes the forensic examination of the **TARGET DEVICE** for the purpose of identifying the electronically stored information described in Attachment B.





**ATTACHMENT B**

1. All records on the **TARGET DEVICE** described in Attachment A that relate to violations of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2), involving ZACHARY WHITE, including but not limited to:
  - a. All voice memos, photographs, videos, audio files, and other audio and video media, and all EXIF information and metadata attached thereto including device information, geotagging information, and information of the dates and times associated with the media;
  - b. All communication records, to include those that have been deleted, including: incoming and outgoing voice messages; text messages; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Facetime, Skype, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
  - c. All information pertaining to contacts, date books, calendars, appointments, or other scheduling records or addresses;
  - d. All information pertaining to stored and/or unretrieved telephone numbers, voice messages, text messages, memorandums, writings, emails, or other communications;
    - i. Any information recording the user's schedule, location, or travel;
    - j. All bank records, checks, credit card bills, account information, and other financial records;
    - k. Evidence of user attribution showing who used or owned the **TARGET DEVICE** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
    - l. All records of Internet Protocol addresses used;
    - m. Evidence of software that would allow others to control the **TARGET DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of data security software designed to detect malicious software;
    - n. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

- o. Evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation; Evidence of the attachment to the **TARGET DEVICE** of other storage devices or similar containers for electronic evidence;
- p. Evidence of programs (and associated data) that are designed to eliminate data from the **TARGET DEVICE**;
- q. Evidence of the times the **TARGET DEVICE** was used;
- r. Passwords, encryption keys, and other access devices that may be necessary to access the **TARGET DEVICE**;
- s. Documentation and manuals that may be necessary to access the **TARGET DEVICE** or to conduct a forensic examination of the **TARGET DEVICE**;
- t. All application date; and
- u. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.